РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

СРБ-ЦЕРТ

Акт о безбедности
информационо-комуникационог система

Оператора ИКТ система

Модел Акта о безбедности ИКТ система представља пример којим су обухваћене све мере заштите предвиђене Законом о информационој безбедности, Уредбом о ближем садржају акта о безбедности ИКТ система од посебног значаја, начину провере и садржају извештаја о провери безбедности ИКТ система од посебног значаја и Уредбом о ближем уређењу мера заштите ИКТ система од посебног значаја. Модел је потребно прилагодити у складу са специфичностима оператора ИКТ Система. Уколико оператор ИКТ система већ има акт којим су прописане неке од мера заштите, у Акту о безбедности наводи назив акта. Иако све мере заштите нису примењиве код свих оператора Актом треба образложити изузимање или смањење обима примене сваке мере појединачно.

Дакле, приликом израде Акта неопходно је дефинисати стварно стање безбедности система и ускладити тренутно стање са препорукама и стандардима предвиђеним Законом и Уредбама. Препорука Националног ЦЕРТ-а је да обавезни чланови радне групе која ће радити на изради Акта буду правници и техничка лица, систем администратори. Важно је истаћи да Акт о безбедности представља документ који је изузетно подложан променама, те је његове одредбе потребно редовно преиспитивати и излагати проверама, а све у циљу стварања што напреднијег нивоа безбедности и изградњи свести запослених и одговорних о значају информационе безбедности ИКТ система.

Значење боја

Црвеном бојом су посебно означени делови текста које сваки оператор мора прилагодити свом ИКТ систему, а у складу са унутрашњом организацијом.

Плавом бојом су дате смернице како би требало да изгледа одређена процедура или упутство којим се детаљније разрађује мера заштите описана у моделу Акта.

На основу члана 8. став 1. Закона о информационој безбедности („Службени гласник РС", број 6/16 и 94/17), чл. 2. и 3. Уредбе о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја („Службени гласник РС", број 94/16), <закона или другог акта којим је основан Оператор ИКТ система, односно којима су дефинисани надлежности, послови и овлашћења>, <одговорно лице или тело> доноси

Акт о безбедности информационо-комуникационог система

< Оператора ИКТ система >

I ОСНОВНЕ ОДРЕДБЕ

Предмет Акта

Члан 1.

Актом о безбедности информационо-комуникационог система < Оператора ИКТ система > (у даљем тексту: Акт о безбедности), у складу са Законом о информационој безбедности („Службени гласник РС", број 6/16 и 94/17, у даљем тексту: Закон), ближе се уређују мере заштите, принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима информационо-комуникационог система < Оператора ИКТ система > (у даљем тексту: ИКТ систем).

Циљеви Акта о безбедности

Члан 2.

Циљеви доношења Акта о безбедности су:

1. одређивање начина и процедура за постизање и одржавање адекватног нивоа безбедности система;
2. спречавање и ублажавање последица инцидената којим се угрожава или нарушава информациона безбедност;
3. подизање свести код запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;
4. прописивање овлашћења и одговорности запослених у вези са безбедношћу и ресурсима ИКТ система;
5. свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите.

Обавеза примене одредби Акта о безбедности

Члан 3.

Мере заштите ИКТ система које су ближе уређене Актом о безбедности служе превенцији од настанка инцидената и минимизацији штете од инцидената и њихова примена је обавезна за све запослене.

Запослени у < Оператору ИКТ система > морају бити упознати са садржином Акта о безбедности и дужни су да поступају у складу са одредбама овог акта, као и других интерних процедура које регулишу информациону безбедност.

< Навести одабране руководеће позиције > одговорни су за праћење примене мера безбедности, као и за проверу да су подаци заштићени на начин који је утврђен овим актом и интерним процедурама.

Одговорност запослених

Члан 4.

Запослени у < Оператору ИКТ система > су дужни да приступају информацијама и ресурсима ИКТ система само ради обављања редовних пословних активности, као и да благовремено информишу овлашћено лице о свим сигурносним инцидентима и проблемима.

Непоштовање одредби Акта о безбедности, као и свако угрожавање или нарушавање информационе безбедности, повлачи дисциплинску одговорност запосленог.

Предмет заштите

Члан 5.

Мере заштите ИКТ система односе се на електронске комуникационе мреже, електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, програмски кôд, податке који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, организациону структуру путем које се управља ИКТ системом, корисничке налоге, тајне информације за проверу веродостојности, техничку и корисничку документацију, унутрашње опште акте и процедуре.

Оператор ИКТ система треба да попише и идентификује имовину коју жели да заштити, те је ово само предлог дефиниције предмета заштите, која ће бити уобличена и конкретизована од стране оператора ИКТ система који доноси акт.

II МЕРЕ ЗАШТИТЕ

Сваки члан садржи опис мера заштите укључујући предлоге процедура, овлашћења и одговорности учесника у спровођењу мера. Уколико су ти описи садржани у другим актима оператора ИКТ система потребно је навести одредбе које упућују на та акта.

Уколико неки од услова није могуће применити или је анализа ризика показала да одређени услов није неопходно применити у пуном обиму, то је потребно образложити у Акту о безбедности.

Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система

Члан 6.

< Оператор ИКТ система > у оквиру организационе структуре утврђује послове и одговорности запослених у циљу управљања информационом безбедношћу.

Интерни акти који уређују обавезе и одговорности запослених у вези са управљањем информационом безбедношћу:

< На пример

- Правилник о унутрашњој организацији и систематизацији радних места;
- Уговори о раду;
- Изјаве о поверљивости;
- Уговори о чувању поверљивости са правним лицима;
- Правилник о приступу посебно осетљивим подацима и информацијама у ИКТ систему.>

< Овлашћени руководилац > је дужан да донесе појединачни акт, у складу са актом о систематизацији, којим одређује одговорна лица за обезбеђивање и праћење безбедности информационог система < Оператора ИКТ система >. Сви запослени морају бити упознати са процедуром заштите безбедности ИКТ система.

< Оператор ИКТ система > <назив посебног акта> утврђује начин доделе овлашћења за приступ ИКТ систему, степен обуке и квалификацију запослених, начин одобравања приступа запосленима од стране руководиоца, односно непосредно надређеног лица. <Посебним актом> утврђује се и одговорност сваког запосленог и одговорног лица и прописује дисциплинска одговорност запосленог, у случају непоштовања одредби које уређују информациону безбедност.

Постизање безбедности рада на даљину и употребе мобилних уређаја

Члан 7.

< Оператор ИКТ система > дозвољава рад на даљину и употребу мобилних уређаја од стране запослених, уколико је осигурана безбедност рада у случају обављања послова ван просторија послодавца, узимајући у обзир и ризике до којих може доћи услед неадекватног коришћења мобилних уређаја.

Уколико оператор не дозвољава рад на даљину, то је потребно навести у ставу 1. овог члана који, ће изостaвити остатак текста везан за ову меру. Такође, предложене мере треба унети у оној мери у којој постоји или је дозвољен рад на даљину и употреба мобилних уређаја.

Рад на даљину

Радни однос за обављање послова ван просторија послодавца обухвата:

- Рад на даљину;
- Рад од куће;
- Виртуелно радно окружење.

Такође, рад на даљину у смислу овог Акта односи се на ситуацију када је запослени и други радно ангажовани обавезан да изврши одређене послове на мрежи послодавца, а налази се ван просторија послодавца.

Предметно ангажовање и омогућавање обављања задатих и неопходних послова се уређује путем Процедуре за VPN приступ информационом систему (у даљем тексту: VPN процедура).

VPN процедура дефинише правила и услове за повезивање на мрежу < Оператора ИКТ система > са удаљене локације. Правилном применом утврђеног поступка и начина приступа, < Оператор ИКТ система > своди на минимум потенцијалну изложеност штети која може настати услед неауторизованог или неконтролисаног приступа мрежи.

VPN процедура се примењује на све запослене у < Оператору ИКТ система > и сараднике који користе рачунаре или мобилне уређаје за повезивање на мрежу < Оператора ИКТ система >, и уређује приступ са удаљених локација у сврху обављања посла у име и за рачун < Оператора ИКТ система >, укључујући коришћење електронске поште и мрежних ресурса, као и начин приступа мрежи < Оператора ИКТ система > са удаљених локација.

Ауторизованим корисницима није дозвољено да користе мрежу < Оператора ИКТ система > за активности које нису у домену пословних активности, радних и других задатака у вези са послом и предметом рада појединачно запосленог.

 # Захтеви који морају бити испуњени и дефинисани у VPN процедури:

1. *Приступ са удаљених локација мора бити заштићен коришћењем криптографских алгоритама.*
2. *Ауторизовани корисници морају чувати креденцијале својих налога и не смеју омогућити приступ било ком трећем лицу.*
3. *Приликом коришћења службеног рачунара за приступ са удаљене локације мрежи* < Оператора ИКТ система >*, ауторизовани корисник не сме истовремено бити повезан и на неку другу мрежу која може угрозити безбедност комуникације.*
4. *Приступ са удаљене локације мора бити одобрен од стране одговорног лица за надзор спровођења VPN процедуре.*
5. *Сви уређаји који су повезани на интерну мрежу преко удаљених локација морају имати инсталирану заштиту у виду антивирусног софтвера. Трећа лица су у обавези да примењују захтеве из закључених уговора са* < Оператором ИКТ система >*.*
6. *Сви пословни подаци који се креирају приликом рада на даљину складиште се у информационом систему. Ради безбедности, пословни подаци се не складиште на мобилним уређајима.*

Рад на даљину запослених или других радно ангажованих (ангажованих за рад у просторијама послодавца) одобрава < назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >.

Коришћење мобилних уређаја

Мобилни уређаји подразумевају све преносне електронске уређаје намењене за комуникацију на даљину. У мобилне уређаје спадају преносиви рачунари, таблети, мобилни телефони, PDA и сви други мобилни уређаји који садржи податке и имају могућност повезивања на мрежу. Приликом коришћења мобилних уређаја потребно је осигурати пословне информације од могућег компромитовања.

< Процедуром о коришћењу мобилних уређаја > дефинише се начин физичке заштитите од крађе и активности које је неопходно предузети у случају крађе или губитка мобилних уређаја, односно безбедносног инцидента, како не би била нарушена безбедност.

< Оператор ИКТ система > спроводи обуку запослених који користе мобилне уређаје, у циљу подизања свести о додатним ризицима до којих долази услед оваквог начина рада.

Процедуром о коришћењу мобилних уређаја потребно је установити следећа правила:

1. *Сви уређаји морају бити заштићени јаком шифром.*
2. *Мора бити инсталирана антивирусна заштита.*
3. *Мора бити усвојена и оперативна процедура за потпуно брисање података када престаје потреба за чувањем истих.*
4. *Крађа или губитак мобилног уређаја се мора без одлагања пријавити надлежној организационој јединици за информационе технологије и одговорном лицу, који затим спроводе активности у смислу очувања безбедности. Уколико се уређај пронађе, потребно је предати исти одговорним лицима.*
5. *Корисницима није дозвољено да врше измене на хардверу или инсталираном софтверу који је власништво* < Оператора ИКТ система > *без претходне писане дозволе сектора за информационе технологије и одговорног лица у сектору.*
6. *У циљу заштите података организациона јединица за информационе технологије ће евидентирати коришћење мобилних уређаја у одговарајућим логовима, које ће у случају потребе користити за истраживања и утврђивања евентуалних злоупотреба.*

Процедура се примењује на све стално запослене, запослене на одређено време или лица ангажована по другим основима, који имају приступ или користе мобилне уређаје у власништву < Оператора ИКТ система >.

Право на коришћење мобилних уређаја ван седишта < Оператора ИКТ система > се стиче на основу писаног захтева корисника мобилног уређаја упућеног организационој јединици за информационе технологије, односно одговорном лицу. Мобилни уређаји који се користе морају бити претходно одобрени и/или набављени од стране < Оператора ИКТ система >, и оцењени као компатибилни са захтевима обезбеђивања адекватног степена заштите.

Рад на даљину може се остварити и коришћењем уређаја који нису мобилни (на пример, десктоп рачунари). Ови уређаји, при томе, морају имати примењене најмање исте безбедносне мере као и сродни уређаји који се налазе у оквиру мреже, док се за заштиту комуникације морају применити исте мере као и за

заштиту комуникације мобилних уређаја. Подешавање ових уређаја врше < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >. Корисници ових уређаја морају обезбедити довољно безбедан простор за њихов рад (засебна соба, положај дисплеја такав да се онемогући посматрање од стране неовлашћених особа и слично).

< Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > одговоран је за вођење евиденције о свим уређајима намењеним за рад на даљину. Евиденција о уређајима треба да садржи податке који су неопходни да би се уређај и/или корисник недвосмислено идентификовали, као што су произвођач, модел, серијски број, инвентарски број, MAC адреса, IMSI, IMEI, корисник који је задужио уређај и његов јединствени матични број и слично.

Корисник мобилног уређаја у обавези је да сваки безбедносни инцидент пријави < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > без одлагања, а у року од < XX > сата да достави писану изјаву о околностима безбедносног инцидента. Под појмом безбедносни инцидент се сматра крађа, губитак мобилног уређаја или било који други догађај који доводи до нарушавања тајности и интегритета података који се налазе на мобилном уређају. < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > је у обавези да, по пријави безбедносног инцидента, неодложно блокира несталом мобилном уређају приступ информационом систему и кориснику промени креденцијале за приступ. У случају да се пронађе мобилни уређај чији нестанак је пријављен, < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > извршиће трајно брисање комплетног медијума за смештање оперативног система, апликација и података и поновну инсталацију оперативног система и потребних апликација. Под појмом „трајног брисања" се сматра процедура брисања података на тај начин да се искључује могућност накнадног повраћаја тих података, а у складу са препоруком *NIST 800-88 Revision 1*.

Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који обављају и у потпуности разумеју своју одговорност

Члан 8.

< Оператор ИКТ система > се стара да запослени који управљају ИКТ системом, односно запослени који користе ИКТ систем имају адекватан степен образовања и способности, као и свест о значају послова које обављају. Њихове одговорности су утврђене < уговором о раду или о ангажовању за рад ван радног односа и интерним актом >.

Провера кандидата и услови запошљавања

< Оператор ИКТ система > спроводи радње у циљу провере испуњености услова сваког појединачног кандидата за запослење, у складу са одговарајућим прописима и етичким правилима, сразмерно пословним захтевима, класификацији информација којима ће имати приступ и сагледаним ризицима.

Сви запослени и радно ангажовани појединци по другом основу којима је додељен приступ поверљивим информацијама, морају потписати споразум о поверљивости и заштити података и информација од трећих лица, пре него што им се дозволи приступ опреми за обраду информација.

Обавезе у току запослења

Руководство < Оператора ИКТ система > је дужно да захтева од свих запослених и радно ангажованих лица да примењују мере заштите безбедности, у складу са овим актом и важећим процедурама.

< Оператор ИКТ система > у циљу развоја, имплементације и одржавања система заштите и безбедности података обезбеђује услове за интеграцију контролних механизама тако што:

- Обезбеђује да се поступци заштите спроводе на организован начин и у складу са процедурама и у континуитету;
- Штити информације и податке са сличним профилом осетљивости и карактеристикама на једнак начин у свим организационим јединицама;
- Спроводи програме заштите на конзистентан и уједначен начин у свим организационим јединицама;
- Координира безбедност и заштиту података у информационом систему са физичком заштитом истих.

< Запослени који су надлежни за праћење, анализу, извештавање и предузимање активности на плану спровођења усвојене политике и процедура > континуирано се обучавају у циљу унапређења техничког и технолошког знања. < Ова лица > су ауторизована за предузимање хитних и неодложних мера у случају постојања непосредне опасности за податке и документацију које су под мерама заштите.

Упознавање са безбедношћу информација, стицање знања и обука

< Сви запослени / одређени запослени > у < Оператору ИКТ система > су у обавези да прођу одговарајућу обуку и редовно стичу нова и обнављају постојећа знања о процедурама које уређују безбедност информација, на начин који одговара њиховом пословном ангажовању и радном месту.

Дисциплински поступак

Дисциплински поступак се спроводи против запослених који су нарушили безбедност информација или на други начин извршили повреду правила и политике на снази и у примени код < Оператор ИКТ система >.

Дисциплински поступак се покреће по предлогу < овлашћеног лица за праћење, прикупљање, анализу и обраду података у односу >.

Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система

Члан 9.

Запослени и по другом основу ангажована лица, дужни су да чувају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система, након престанка или промене радног ангажовања. Дужности и обавезе које остају важеће и после престанка ангажовања и треба да буду садржане у тексту уговора о раду са запосленим и у условима заснивања радног односа, односно уговора о ангажовању лица ван радног односа.

Ова мера је ближе одређена:

<

- Процедуром о правима приступа информационом систему
- Уговором о раду
- Уговором о ангажовању лица ван радног односа
- Споразумом о поверљивости >

За поступања приликом престанка запослења или ангажовања задужен/а је < служба за људске ресурсе или надређени руководилац или организациона јединица за информационе технологије >, који предузимају следеће активности:

<

- проверава испуњеност свих услова у погледу чувања и изношења података у електронском и папирном формату,
- прегледа све налоге и приступе систему који су били доступни запосленом,
- преузима од запосленог електронске и друге мобилне уређаје,
- утврђује начин контакта са бившим запосленим након одласка,
- проверава враћене мобилне уређаје и уређаје за преношење података,
- даје налог за укидање налога електронске поште и свих других права приступа систему < Оператора ИКТ система > на дан престанка радног односа или другог основа ангажовања бившег запосленог,
- прегледа све налоге за приступ одлазећег запосленог и прикупља приступне шифре и кодове са циљем укидања/промене истих на дан одласка,
- преузима картице или друге уређаје којима се омогућава приступ пословним просторијама и опреми < Оператора ИКТ система >.

Идентификовање информационих добара и одређивање одговорности за њихову заштиту

Члан 10.

Информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компоненти, техничку и корисничку документацију, унутрашње опште акте и процедуре.

Пописивање имовине

< Оператор ИКТ система > врши идентификацију имовине која одговара животном циклусу информација и документује њен значај. Животни циклус информације обухвата креирање, обраду, складиштење, пренос, брисање и уништавање података и информација. < Оператор ИКТ система > прави попис добара који је тачан, ажуран, конзистентан и усклађен са другом имовином.

Евиденцију о информационим добрима и средствима и имовини за обраду информационих добара води < назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >.

Власништво над имовином, прихватљиво коришћење имовине и њен повраћај

Појединци којима је дата одговорност за контролисање животног циклуса имовине дужни су да правилно управљају имовином током целог животног циклуса.

< Оператор ИКТ система > у оквиру < интерног акта о руковању имовином > уређује правила за прихватљиво коришћење имовине повезане са информацијама и опремом за обраду информација.

Запослени и екстерни корисници су обавезни да врате сву имовину < Оператора ИКТ система > коју поседују након престанка њиховог запослења, уговора или споразума о ангажовању на одређеним пословима и задацима.

Током отказног рока запослених, < Оператор ИКТ система > контролише њихово неовлашћено копирање, умножавање или преузимање релевантних заштићених информација.

Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. Закона о информационој безбедности

Члан 11.

Класификовање података је поступак утврђивања и појединачног додељивања нивоа тајности података, у складу са њиховим значајем за < Оператор ИКТ система >.

< Оператора ИКТ система > означава типове и локације података као поверљиве, интерне или јавне. Имовина се означава уз помоћ идентификационих налепница које носе одговарајућу класификациону ознаку.

< Оператор ИКТ система > класификациону шему поверљивости информација базира на четири нивоа:

<

- откривање не изазива никакву штету;
- откривање изазива мању непријатност или мању штету;
- откривање има значајан краткорочни утицај на пословање или тактичке циљеве;
- откривање има озбиљан утицај на дугорочне стратешке циљеве или угрожава опстанак. >

< Оператор ИКТ система > врши класификацију ради:

- Јачања корисничке одговорности, како би корисници могли да уоче и препознају пословну вредност података приликом чувања или слања и постану свесни одговорности за неовлашћено коришћење или преношење;
- Подизања свести о вредности информације или документа;
- Заштите података у покрету ради боље и интелигентније интеграције са DLP, WEB gateway и осталим производима за заштиту параметара и крајњих уређаја;
- Заштите садржаја;
- Интеграције са системима за архивирање.

Класификација документа мора да буде усклађена са правилима контроле приступа.

< Оператор ИКТ система > поступања у складу са усвојеном Шемом класификовања података. Посебном процедуром се дефинишу радње за поступање, обраду, складиштење и пренос података.

 # Процедура о поступању са имовином мора да подразумева:

- ограничења приступа која подржавају захтеве за заштиту сваког нивоа класификације;
- одржавање званичног записа о овлашћеним примаоцима имовине;
- заштиту привремених или трајних копија података на нивоу који је у складу са заштитом оригиналне информације;
- складиштење информационе имовине у складу са спецификацијама произвођача;
- јасно обележавање свих копија медија на које овлашћени прималац треба да обрати пажњу.

Заштита носача података

Члан 12.

<Оператор ИКТ система> обезбеђује спречавање неовлашћеног откривања, модификовања, уклањања или уништења података који се чувају на носачима података.

Евиденцију носача на којима су снимљени подаци, води < назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >.

Управљање преносним носачима података (медијума)

<Оператор ИКТ система> је дужан да развија и имплементира процедуру о управљању преносним носачима, у складу са усвојеном Шемом класификовања података.

 # Процедура о управљању преносним носачима може садржати следеће одредбе:

- *садржај сваког медијума који се може поново користити и који ће се износити изван организације, онда када више није потребан, треба да се неповратно избрише;*
- *за све медијуме који се износе из организације, онда када је то неопходно и изводљиво, треба захтевати одобрење, а о свим таквим изношењима треба водити евиденцију, како би се сачувао траг за проверу;*
- *све медијуме треба складиштити на безбедном и заштићеном месту, у складу са препорукама произвођача;*
- *коришћење криптографских техника за заштиту података на преносним медијумима, ако су поверљивост или интегритет података важни;*
- *подаци треба да буду пренети на нови медијум пре него што постану нечитљиви;*
- *вишеструке копије вредних података треба чувати на одвојеним медијумима да би се додатно смањио ризик од случајног оштећења или губитка података;*
- *да би се ограничила могућност губљења података, треба предвидети регистровање преносних медијума;*
- *покретне преносне медијуме треба користити само ако за то постоји пословна потреба;*

- *уколико постоји пословна потреба за коришћењем преносних медијума, неопходно је пратити пренос података на такве медијуме.*

Расходовање носача података (медијума)

Када више нису потребни, медијуми су расходују на безбедан начин, применом Процедуре за безбедно расходовање медијума.

Расходовање медијума на безбедан начин < Оператор ИКТ система > врши свођењем на минимум ризика од могућег преузимања осетљивих података од стране неовлашћених особа.

Процедуром за безбедно расходовање медијума који садрже поверљиве податке утврђују се различити начини процеса расходовања, а у складу са осетљивошћу података.

 # Процедура за безбедно расходовање медијума даје следеће смернице:

- *неопходно је уредити начин за идентификовање медијума који садрже осетљиве податке за које ће можда бити потребно безбедносно расходовање;*
- *медијуме који садрже осетљиве податке треба расходовати спаљивањем или кидањем, или брисањем података ради коришћења у неком другом апликативном програму унутар организације;*
- *расходовање медијума који садрже осетљиве податке је потребно евидентирати, како би се сачувао траг за проверу.*

Физички пренос носача података (медијума)

Носачи података који садрже информације се штите од неовлашћеног приступа, злоупотребе или оштећења приликом транспорта. Када поверљива информација на медијуму није шифрована, потребно је додатно физички заштити медијум.

 # Смернице за безбедан транспорт:

- *користити поуздани транспорт или курире;*
- *потребно је увести проверу идентитета курира;*
- *карактеристике опреме за пренос морају да буду такве да обезбеде заштиту од свих физичких оштећења која би могла настати током преноса.*

У случају транспорта носача података са информацијама, < назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > одређује лице које ће вршити транспорт и начин транспорта.

Ограничење приступа подацима и средствима за обраду података

Члан 13.

Подацима и средствима за обраду података је неопходно ограничити приступ у складу са утврђеним степеном тајности података и усвојеном Шемом класификовања података према члану 11. овог акта.

< Оператор ИКТ система > ће формирати Контролну листу приступа која садржи попис свих информационих објеката и субјекте који им могу приступити.

Корисницима је дозвољен приступ само мрежи и мрежним услугама за чије коришћење су овлашћени.

< Оператор ИКТ система > ће посебним документом уредити приступ мрежи и мрежним уређајима.

#Садржај процедуре о приступу мрежи и мрежним уређајима:

- *листа мрежа и мрежних услуга којима је приступ дозвољен;*
- *начини ауторизације ради утврђивања коме је одобрен приступ, којој мрежи и којим услугама;*
- *начин управљања заштитом приступа мрежним прикључцима и услугама;*
- *средства која се користе за приступ мрежама и мрежним услугама;*
- *захтеви у погледу верификације корисника за приступ различитим мрежним услугама;*
- *начини надгледања коришћења мрежних услуга.*

Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа

Члан 14.

< Оператор ИКТ система > управља приступом ИКТ систему и услугама кроз употребу корисничких идентификатора.

< Управљање корисничким идентификаторима врши се уз поштовање следећих принципа:

- кориснички идентификатори су јединствени, тако да се корисници могу везати уз њих и учинити одговорним за своје активности;
- коришћење заједничких идентификатора дозвољава се само онда када је то погодно за обављање посла уз претходно одобрење;
- корисницима којима је престао радни однос или период ангажовања тренутно се онемогућавају или уклањају кориснички идентификатори;
- периодично идентификовање и уклањање или онемогућавање вишеструких корисничких идентификатора;
- вишеструки идентификатори неког корисника се не издају другим корисницима.>

Сваком кориснику се додељује право приступа ИКТ систему у складу са радним задацима које обавља. Кориснику се додељују јединствени подаци за логовање и јединствена шифра за логовање, који се не смеју делити са другим корисницима.

Додељивање привилегованих (администраторских) права на приступ врши се на основу < одлуке одговорног лица >.

< Привилегована права на приступ додељују посебно за сваки системски објекат уз дефинисан рок трајања тих права >.

Привилегована права на приступ која треба доделити корисничком идентификатору другачија су од оних која се користе за редовне активности. Редовне пословне активности не треба вршити из привилегованих корисничких идентификатора. Компетенције корисника са привилегованим правима на приступ се редовно преиспитују ради провере да ли су у складу са њиховим обавезама.

Забрањено је неовлашћено коришћење општих корисничких идентификатора администратора.

Шифре за приступ општим корисничким идентификаторима администратора се мењају променом корисника.

< Оператор ИКТ система > *< једном годишње >* врши преиспитивање права корисника на приступ, као и након сваке промене (унапређење, разрешење и крај запослења).

Запосленима, другим радно ангажованим и екстерним корисницима информација и опреме за обраду информација по престанку запослења или истеку уговора укида се право на приступ.

Утврђивање одговорности корисника за заштиту сопствених средстава за аутентификацију

Члан 15.

Аутентификације корисника којима је одобрен приступ систему врши се путем <јединственог корисничког имена и шифре>.

Сви корисници су дужни да:

- < корисничко име и шифру > држе у тајности, не откривају их другим лицима, укључујући и надређене особе;
- избегавају чување < корисничког имена и шифре > у писаном облику;
- промене < шифру > када примете да постоји било какав наговештај могућег компромитовања.

<Шифре морају да:

- Садрже најмање 9 алфанумеричких карактера;
- Садрже најмање једно велико и једно мало слово;
- Садрже најмање 1 број (0-9).

Шифре не заснивати на личним подацима корисника, као што су име, телефонски број или датум рођења и не смеју садржати више од 3 узастопна идентична бројчана или словна знака.

Корисници су дужни да привремене шифре промене приликом првог пријављивања.>

Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података

Члан 16.

У циљу заштите података <Оператор ИКТ система> развија и имплементира политику коришћења криптографских контрола, и успоставља механизме и систем за управљање кључевима.

< Криптозаштита обезбеђује:

- Аутентификацију (идентификацију корисника и других системских ентитета који захтевају приступ или одобрење акције корисника);
- Непорецивост (примена криптографских техника, најчешће дигиталног потписа, како би се добила потврда о извршавању или неизвршавању неке акције од стране појединачног корисника);

- Поверљивост (применом шифровања врши се заштита осетљивих или критичних информација које се складиште или преносе);
- Интегритет (непроменљивост података који се преносе).

Поступак криптографске контроле обухвата:

- анализу и процене потреба примене криптографије у пословним процесима укључујући опште принципе према којима би пословне информације требало да се штите;
- ниво заштите се одређује узимањем у обзир типа алгоритма за криптовање података, јачине и квалитета криптографског алгоритма;
- примену шифровања за заштиту осетљивих података приликом преноса мобилним или другим медијумима, уређајима или преко комуникационих водова;
- управљање кључевима (заштита криптографских кључева, повраћај шифрованих података у случају губљења, компромитовања или оштећења кључева). >

Управљање кључевима

< Оператор ИКТ система > примењује следеће методе за управљање кључевима које обухватају њихов цео животни циклус:

- генерисање кључева;
- издавање и добијање сертификата за јавне кључеве;
- складиштење кључева (кључеви се чувају на посебним уређајима или паметним картицама, на месту које је физички обезбеђено);
- дистрибуцију кључева (додела кључева намењеним ентитетима и активација самог кључа);
- замену или ажурирање кључева;
- поступак у случају компромитовања кључева;
- деактивацију кључева;
- обнављање изгубљених или оштећених кључева;
- прављење резервних копија или архивирање кључева;
- уништавање кључева;
- евидентирање и проверу активности у вези са управљањем кључевима.

Кључеви се могу користити само у периоду који одреди <одговорно лице>.

Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему

Члан 17.

< Оператор ИКТ система > је дужан да предузме мере ради спречавања неовлашћеног физичког приступа < објекту, простору, просторијама, зони >, у којима се налазе средства и документи ИКТ система, као и спречавање оштећења и ометања информација.

Зона раздвајања и успостављање система физичке безбедности

Опрема за обраду информација се штити закључавањем просторија у којима се налази.
У складу са проценом ризика дефинисане су следеће зоне раздвајања: < >.

#Шта су зоне раздвајања?

- *зоне раздвајања у згради или на локацији која садржи опрему за обраду информација треба да буду физички исправне (тј. не треба да постоје процепи у зони или области у којој би се лако могао десити упад); спољни кров, зидови и подови на тој локацији треба да буду од чврстог материјала, а сва спољна врата треба да буду потпуно заштићена од неовлашћеног приступа помоћу контролних механизама, нпр. решеткама, алармима, бравама итд.; врата и прозори треба да буду закључани у свим случајевима када су без надзора, а када су у питању прозори, треба размотрити спољну заштиту, посебно у приземљу;*
- *треба поставити пријавнице са особљем или друга средства за контролу физичког приступа до локације или зграде; приступ локацијама или зградама треба да буде ограничен само на овлашћено особље;*
- *онда када је то применљиво, треба да буду изграђене физичке препреке како би се спречио неовлашћени физички приступ и загађење из околине;*
- *сва пожарна врата у безбедносној зони раздвајања треба да имају алармни уређај, да буду под надзором и да се испитују на споју са зидовима како би се успоставио потребан ниво отпорности у складу са одговарајућим регионалним, националним и међународним стандардима; треба да функционишу у складу са локалним противпожарним правилима у погледу осигурања од отказа;*
- *да би се надгледала сва спољна врата и доступни прозори, треба поставити погодне противпровалне алармне системе у складу са националним, регионалним или међународним стандардима; области без особља треба да буду под алармом у сваком тренутку; надзор треба такође обезбедити и за друге области, нпр. за просторију са рачунарима или за просторије за комуникације;*
- *опрема за обраду информација којом управља организација треба да буде физички одвојена од оне којом управљају трећа лица.*

Контрола физичког уласка

Безбедносне области морају бити заштићене одговарајућим контролама уласка како би се осигурало да је само овлашћеним појединцима дозвољен приступ, складу са смерницама.

#Смернице за контролу физичког уласка:

- *евиднетирати датуме и време уласка и изласка посетилаца, а све посетиоце треба надгледати, осим ако њихов приступ није претходно одобрен; приступ треба одобравати само за специфичне, ауторизоване сврхе и издавати упутства о захтевима за безбедност области и о процедурама за ванредне ситуације;*
- *приступ областима у којима се обрађују или чувају поверљиве информације треба да буде ограничен само на овлашћене особе, применом одговарајућих контрола приступа, нпр. имплементацијом двофакторских механанизама за проверу веродостојности, као што су картице за приступ и тајни лични идентификациони број (PIN);*

- *треба безбедно одржавати и надгледати евиденцију или електронску проверу свих приступа;*
- *од свих запослених, уговарача и треће стране, као и од свих посетилаца треба захтевати да носе видљиву идентификацију и да известе особље обезбеђења уколико наиђу на посетиоце без пратиоца или примете особу која не носи видљиву идентификацију;*
- *запосленима код пружаоца услуга обезбеђења треба одобрити ограничен приступ безбедосним областима или опреми за обраду осетљивих података и омогућити када за то постоји потреба; овакав приступ треба да буде одобрен и надгледан у сваком тренутку;*
- *права приступа безбедносним областима треба редовно преиспитивати и ажурирати, а уколико постоји потреба и укинути.*

Заштита канцеларија, просторија, средстава, као и заштита од претњи екстерних фактора из окружења

< Оператор ИКТ система > обезбеђује и примењује одговарајућу контролу приступа, чиме се омогућава физичка безбедност канцеларија, просторија и средстава. Такође, безбедним конфигурисањем се онемогућава приступ кључној опреми а у циљу спречавања видљивости поверљивих информација, активностима споља. Физичка заштита се мора планирати и за случајеве природних катастрофа, непријатељских напада или несрећа.

Рад у безбедносним зонама

< Безбедносне зоне подлежу следећим мерама заштите:

- особље мора бити обавештено о активностима унутар безбедносне зоне;
- забрањује се рад без надзора у безбедносним зонама;
- безбедносне зоне које се не користе морају бити физички закључане и чија провера се врши периодично;
- не дозвољава се уношење фотографских, видео, аудио или других уређаја за записивање, осим уз претходно одобрење одговорног лица. >

Евиденцију о уласку у безбедносну зону < назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >.

Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем

Члан 18.

Постављање и заштита опреме

Опрема се поставља и штити на начин којим се смањује ризик од претњи и опасности из окружења, као и могућношћу неовлашћеног приступа.

#Смернице за безбедност опреме:

- Опрема се поставља на месту које се може обезбедити од неовлашћеног приступа;
- Опрема за обраду информација која служи за приступ и коришћење осетљивих података се поставља не места која нису видљива неовлашћеним особама;

- Врши се редовна контрола система за обезбеђење, аларма, противпожарне заштите, као и инсталација за воду, струју, гас, електронске комуникације;
- Просторије са опремом треба редовно чистити од прашине;
- Забрањено је конзумирање хране и пића и пушење близини опреме за обраду информација;
- Редовно се прате температура и влажност ваздуха;
- Опрема мора бити заштићена од атмосферских падавина;
- Опрема у индустријском окружењу се штити применом специјалних метода заштите.

< Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > редовно прати услове околине, као што су температура и влажност, који би могли негативно да утичу на рад опреме за обраду информација.

Помоћне функције за подршку

Опрема се штити од прекида напајања, тако што се:

- помоћна опрема за напајање одржава у складу са спецификацијама опреме произвођача и прописима;
- капацитет помоћне опреме редовно процењује;
- редовно прегледа и испитује у погледу правилног функционисања и врши поправка кварова;
- обезбеђује вишеструко напајање са различитих траса.

Безбедносни елементи приликом постављања каблова

Каблови за напајање и телекомуникациони каблови који преносе податке или који представљају подршку информационим услугама штите се од прислушкивања, ометања или оштећења на следећи начин:

- водови напајања и телекомуникациони водови који улазе у просторије за обраду информација су подземни, онда када је то могуће, или имају адекватну алтернативну заштиту;
- каблови за напајање се одвајају од комуникационих каблова да би се спречиле сметње;
- за осетљиве или критичне системе се постављају оклопљени водови, користе се закључане просторије или кутије и примењује се електромагнетско оклапање ради заштите каблова;
- неовлашћено прикључење уређаја на каблове се врши техничким претраживањем и физичком провером;
- приступ до разводних табли и у просторије са кабловима се контролише.

Одржавање опреме

Опрема се одржава како би се осигурали њена непрекидна расположивост и неповредивост, и то на следећи начин:

- опрема се одржава у складу са препорученим сервисним интервалима и према спецификацијама које је дао испоручилац;

- поправке и сервисирање опреме обавља само особље овлашћено за одржавање;
- о свим сумњивим или стварним неисправностима, као и о целокупном превентивном и корективном одржавању се чувају записи;
- осетљиве информације треба избрисати из опреме;
- пре враћања опреме у рад након одржавања, потребно је прегледати како би проверили да није неовлашћено коришћена или оштећена.

Измештање и премештање имовине

Опрема, информације или софтвер се измештају само уз одобрење одговорног лица, а током измештања се примењују следећа правила:

- треба да се одреде запослени и спољни корисници који имају овлашћење да одобре измештање имовине;
- треба да се поставе временска ограничења за измештање опреме и да се проверава усклађеност приликом повратка;
- треба документовати идентитет и улогу лица која користе или поступају са имовином приликом премештања и ова документација треба да буде враћена са опремом, информацијама или софтвером.

Безбедност измештене опреме и имовине

На измештену опрему треба применити безбедносне механизме заштите, узимајући у обзир различите ризике приликом рада изван просторија.

Безбедно расходовање или поновно коришћење опреме

Сви делови опреме који садрже медијуме за чување података потребно је верификовати да би се осигурало да су сви осетљиви подаци и лиценцирани софтвери пре расходовања или поновног коришћења безбедно уклоњени.

Безбедност опреме корисника без надзора

Корисници треба да обезбеде да опрема која је без надзора има одговарајућу заштиту, у циљу онемогућавања приступа заштићеним информацијама и подацима.

Остављање осетљивих и поверљивих докумената и материјала

Сва осетљива и поверљива документа и материјали морају да буду уклоњени са радне површине и одложени на одговарајуће место које се закључава, у периоду када запослени није присутан на свом радном месту или када се документа и материјали не користе.

#Процедура:

1. *Све осетљиве и поверљиве информације у штампаном или електронском облику запослени морају одложити на сигурно место на крају радног дана или када нису присутни на свом радном месту.*
2. *Рачунари морају бити закључани у одсуству запосленог и угашени на крају радног дана.*
3. *Ормари и фиоке у којима се чувају поверљиви подаци морају бити закључани када се не користе, а кључеви не смеју бити остављени на приступачном месту без надзора.*
4. *Лаптопови морају бити везани уз помоћ одговарајуће опреме или закључани у фиоци. Таблети и остали преносни уређаји морају бити закључани у фиоци.*
5. *Носачи података као што су дискови и flash меморија морају бити одложени и закључани.*
6. *Шифре за приступ не смеју бити написане и остављене на приступачном месту.*
7. *Штампани материјал који садржи осетљиве информације се мора одмах преузети са штампача приликом штампања.*
8. *Материјал који је намењен за бацање треба уништити или одложити на место које се закључава, а које је намењено за одлагање такве врсте материјала.*

Обезбеђивање исправног и безбедног функционисања средстава за обраду података

Члан 19.

У циљу обезбеђивања исправног и безбедног функционисања средстава за обраду података, дефинишу се процедуре за руковање средствима, које се односе на отпочињање и завршетак приступа информационом систему, прављење резервних копија, одржавање опреме, руковање носачима података, контролу приступа у просторије са серверском инфраструктуром, комуникационом опремом и системима за складиштење података, као и у случајевивма измештања делова ИКТ система. Усвајање и примена радних процедура.

< Оператор ИКТ система > успоставља радне процедуре које садрже инструкције за детаљно извршење следећих послова:

а) инсталација и конфигурација система;

б) обраду и поступање са информацијама (аутоматски и мануелно);

в) израда резервних копија;

г) обрада захтева за временски распоред активности;

д) израда инструкција за поступање у случају грешке или у другим ванредним ситуацијама која могу да настану у току извршавања посла, укључујући ограничења у коришћењу системских помоћних функција;

ђ) утврђивање листе контаката за подршку и есклацију (укључујући екстерне контакте за подршку) у случају неочекиваних оперативних или техничких потешкоћа;

е) израда инструкција за управљање поверљивим подацима;

ж) процедуре за поновно покретање система и опоравак, које се користе у случају отказа система;

з) управљање системским записима (логовима);

и) процедуре за надгледање.

За усвајање, измене и допуне радних процедура овлашћен је < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >.

Управљање расположивим капацитетима

Коришћење ресурса се континуирано надгледа, подешава и пројектује у складу са захтеваним капацитетима, како би се осигурале неопходнеперформансе система. Периодично се спроводе следеће активности:

а) брисање застарелих података;
б) повлачење из употребе апликација, система, база података или окружења;
в) оптимизација серије процеса и распореда;
г) одбијање или ограничавање пропусног опсега услуга захтеваних у погледу ресурса, ако оне нисукритичне за пословање.

Раздвајање окружења за развој, испитивање и рад

Окружења за развој, испитивање и рад су међусобно раздвојена, како би се смањио ризик од неовлашћеног приступа или промена у радном окружењу.

#Смернице:

а) треба дефинисати и документовати правила за преношење софтвера из развојног статуса у оперативни статус;
б) развојни и оперативни софтвери треба да се извршавају на различитим системима илирачунарским процесорима, као и у различитим доменима или директоријумима;
в) промене у оперативним системима и апликацијама треба испитивати у окружењу за испитивање или режиму одржавања пре него што се примене на оперативне системе;
г) испитивање не треба да се ради на оперативним системима, осим у изузетним околностима;
д) компајлери, едитори и други развојни алати или системски помоћни програми не треба да буду доступни из оперативних система, ако се то не захтева;
ђ) да би се смањио ризик од грешке, корисници треба да примењују различите корисничке профиле за оперативне и системе за испитивање, а менији треба да приказују одговарајуће идентификационе поруке;
е) осетљиве податке не треба копирати у системско развојно окружење, осим ако нису обезбеђене еквивалентне контроле за систем за испитивање.

За обезбеђивање исправног и безбедног функционисања средстава за обраду података и примену радних процедура задужен је < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >.

Заштита података и средстава за обраду података од злонамерног софтвера

Члан 20.

Злонамерни софтвер обухвата све програме који су направљени у намери да отежају рад или оштете неки умрежен или неумрежен рачунар. Заштита од злонамерног софтвера се заснива на софтверу за

откривање злонамерног софтвера и отклањање штете, на познавањуинформационе безбедности, као и на одговарајућим контролама приступа систему и управљању захтеваним и потребним променама.

Поступак контроле и предузимање мера против злонамерног софтвера

< Оператор ИКТ система > одређује и примењује контроле откривања, спречавања и опоравка, ради заштите од злонамерног софтвера.

#Садржај процедуре о заштити од злонамерног софтвера:

1. *формална забрана коришћења неауторизованих софтвера;*
2. *имплементација контрола које спречавају или откривају коришћење неовлашћеног софтвера;*
3. *имплементација контрола које спречавају или откривају коришћење познатих или сумњивих компромитованих веб-сајтова;*
4. *успостављање формалне политике ради заштите од ризика повезаних са добијањем датотека и софтвера од или преко спољних мрежа, или на било ком другом медијуму, указујући на то које заштитне мере треба предузети;*
5. *смањење рањивости које може да експлоатише непријатељски софтвер, нпр. кроз управљање техничким рањивостима;*
6 *спровођење редовних преиспитивања софтвера и садржаја података у системима који подржавају критичне пословне процесе; присуство било каквих неодобрених датотека или неауторизованих допуна треба формално истражити;*
7. *инсталирање и редовно ажурирање софтвера за откривање злонамерног софтвера и опоравак ради претраживања рачунара и медијума као контролу из предострожности, или на рутинској основи.*

#Листа провера које се спроводе:

а) проверу, пре коришћења, свих датотека на електронским или оптичким медијумима, као и датотека примљених преко мрежа, да ли садрже злонамерни софтвер;

б) проверу, пре коришћења, садржаја прилога електронске поште и преузетих садржаја, да ли садрже злонамерни софтвер; ову проверу треба спроводити на разним местима, нпр. на серверима за електронску пошту, на стоним рачунарима или приликом уласка у мрежу оператора ИКТ система;

в) проверу постојања злонамерних софтвера на веб-страницама;

г) дефинисање процедура за менаџмент и одговорности за поступање са заштитом од злонамерног софтвера у системима, обука за њихово коришћење, извештавање и опоравак од напада злонамерним софтвером;

д) припрему одговарајућих планова за континуитет пословања приликом опоравка од напада злонамерним софтвером, укључујући све неопходне резервне копије података и софтвера и механизме за опоравак;

ђ) имплементацију процедура за редовно прикупљање информација, као што је претплата на адресне спискове за доставу или провера веб-страница на којима се дају информације о новим злонамерним софтверима;

е) имплементацију процедура за верификовање информација о злонамерним софтверима и обезбеђење да су упозоравајући извештаји тачни и информативни; руководиоци треба да осигурају да се за разликовање лажних од стварних злонамерних софтвера користе квалификовани извори,

нпр. проверени часописи, поуздане странице на Интернет мрежи или испоручиоци програма против злонамерних софтвера; сви корисници треба да буду свесни проблема појаве духовитих или злонамерних обмана и онога што треба да раде после њиховог пријема.

Препоручује се доношење и процедуре о антивирусној заштити и процедуре о подизању свести запослених о информационој безбедности.

У случају да корисник примети необично понашање рачунара, запажање треба без одлагања да пријави < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >.

У циљу заштите одупада у ИКТ систем, < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > је дужан да одржава систем за спречавање упада.

Корисницима који су прикључени на ИКТ систем у случају доказане злоупотребе Интернета < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > може укинути приступ.

Заштита од губитка података

Члан 21.

< Оператор ИКТ система > врши израду резервних копија које обухватају системске информације, апликације и податке који су неопходни за опоравак целокупог система у случају наступања последица изазваних ванредним околностима.

Резервне копије информација и података

Резервне копије информација, софтвера и дупликати система се редовно израђују и испитују.

Заштитне копије корисницима обезбеђују корисничке податке, функционалност сервиса и апликација након уништења или оштећења која су настала услед хакерских напада, отказа хардвера, грешака корисника, природних катастрофа и других несрећа.

Под заштитним копијама подразумева се прављење резервних копија корисничких података, конфигурационих и *log* фајлова, критичних фајлова за функционисање оперативних система (серверских, корисничких и комуникационих) или целих оперативних система, апликација, сервиса и базе података.

Заштитне копије треба да омогуће брзо и ефикасно враћање у функцију система у случају нежељених догађаја, и треба их правити у време када се не умањује расположивост сервиса, апликација, база података и комуникационих капацитета ИКТ система.

За чување заштитних копија користе се магнетне траке, екстерни хард дискови и CD/DVD медији.

< Надлежна организациона јединица за ИТ извршава следеће задатке:

- процењује осетљиве и критичне податке за које је потребно правити резервне копије;
- креира план прављења резервних копија;
- прави заштитне копије серверског оперативног система и података, комуникационог оперативног система и конфигурационих фајлова, апликација, сервиса и база података;
- верификује успешно прављење резервних копија;
- води евиденцију урађених резервних копија;

- одлаже копије на безбедно место;
- тестира исправност резервних копија и процедуре за прављење заштитних копија;
- рестаурира податке са резервних копија. >

#План израде резервних копија информација обухвата следеће:

- *тачне и потпуне записе о резервним копијама и документоване процедуре обнављања;*
- *обим и учесталост израде резервних копија;*
- *резервне копије треба да одражавају пословне потребе организације и критичност тих информација по континуитет пословања организације;*
- *треба их складиштити на локацији на довољној удаљености, како би се избегло свако оштећење на главној локацији;*
- *резервним копијама информација треба дати одговарајући ниво физичке заштите и заштите од утицаја околине (описано у тачки 12) који је доследан мерилима која се примењују на главној локацији;*
- *медијуме са резервним копијама треба редовно проверавати, ради сигурности њихове употребе у ванредним ситуацијама и када је то неопходно;*
- *у ситуацијама у којима је важна поверљивост, резервне копије треба заштитити помоћу шифровања.*

За заштиту од губитка података одговоран је < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >.

Чување података о догађајима који могу бити од значаја за безбедност ИКТ система

Члан 22.

У ИКТ систему < Оператора ИКТ система > формирају се записи о догађајима (логови) у вези са активностима корисника, грешкама и догађајима у вези са информационом безбедношћу.

Записивање догађаја

< Оператор ИКТ система > прави записе о догађајима и бележи активности корисника, грешке и догађаје у вези са -информационом безбедношћу, који се морају чувати и редовно преиспитивати. < Администратори система немају дозволу да бришу или деактивирају дневнике о сопственим активностима. >

Записи о догађајима садрже:

- идентификаторе корисника;
- активности система;
- датуме, време и детаље кључних догађаја, нпр. пријављивања и одјављивања;
- идентитет или локацију уређаја, ако је могуће, и идентификатор система;
- записе о успешним и одбијеним покушајима приступа систему;
- записе о успешним и одбијеним покушајима приступа подацима и другим ресурсима;
- промене у конфигурацији система;
- коришћење привилегија;

- коришћење системских помоћних функција и апликација;
- датотеке којима се приступало и врсте приступа;
- мрежне адресе и протоколе;
- аларме које је побудио систем за контролу приступа;
- активирање и деактивирање система заштите, као што су антивирусни системи и системи за откривање упада.

Заштита информација у записима

Средства за записивање и записане информације су заштићени од неовлашћеног мењања и приступа.

Забрањено је неовлашћено уношење следећих измена:

- мењање типова порука које се записују;
- уношење измена у датотеке са записима или њихово брисање;
- препуњавање медијума за записе, што доводи до отказа записивања догађаја или уписивања преко већ раније записаног.

Записи администратора и оператора

Активности администратора и оператора система се записују, а записи штите и редовно преиспитују. Власници привилегованих корисничких налога могу бити у стању да управљају записима на опреми за обраду информација која је под њиховом директном контролом, на који начин се штите и прегледају записи да би се одржала одговорност за привилеговане кориснике.

Сатови свих одговарајућих система за обраду информација заштите морају бити синхронизовани по Гриничком средњем времену.

За чување података о догађајима који могу бити од значаја за безбедност ИКТ система задужен је < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >.

Обезбеђивање интегритета софтвера и оперативних система

Члан 23.

< Оператор ИКТ система > спроводи процедуре којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система, у складу са смерницама за контролу промена и инсталацију софтвера.

#Смернице за контролу промена и инсталацију софтвера

- *ажурирање оперативног софтвера, апликација и програмских библиотека могу да обављају само оспособљени администратори, по добијању одговарајућег овлашћења од руководиоца;*
- *оперативни системи треба да садрже само одобрене извршне кодове, а не и развојне кодове или компилаторе;*
- *апликације и оперативни системски софтвер треба имплементирати тек после обимног и успешно спроведеног испитивања, које обухвата испитивање применљивости, безбедности, утицаја на друге системе и погодности за коришћење, а треба их спроводити на засебним системима, односно тест-ним окружењима (описано у тачки ... тестирање);*

- *треба осигурати да су све одговарајуће библиотеке изворних програма ажуриране;*
- *пре имплементације било каквих промена, треба успоставити стратегију повратка на претходно стање;*
- *приликом свих ажурирања на библиотекама оперативних програма, треба одржавати записе за проверу;*
- *као меру предострожности за неочекиване ситуације треба сачувати претходне верзије апликативног софтвера;*
- *старије верзије софтвера треба архивирати, заједно са свим потребним информацијама и параметрима, процедурама, детаљима конфигурације и софтвером за подршку, све док се подаци држе у архиви.*

Инсталацију и подешавање софтвера може да врши само < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >, односно запослени-корисник који има овлашћење за то.

Заштита од злоупотребе техничких безбедносних слабости ИКТ система

Члан 24.

< Оператор ИКТ система > врши анализу ИКТ система и утврђује степен изложености ИКТ система потенцијалним безбедносним слабостима, и предузима одговарајуће мере које се односе на уклањање препознатих слабости или примену мера заштите.

Управљање техничким рањивостима

< Оператор ИКТ система > благовремено прикупља информације о техничким рањивостима информационих система који се користе, вреднује изложеност тим рањивостима и предузима одговарајуће мере, узимањем у обзир припадајућих ризика.

Посебне информације које су потребне за подршку управљања техничким рањивостима обухватају продавца софтвера, бројеве верзија, текуће стање размештаја, као и особе које су одговорне за тај софтвер.

#Смернице:

- < Оператор ИКТ система > *дефинише и успоставља улоге и одговорности у вези са управљањем техничким рањивостима, укључујући надзор, оцену ризика услед утврђене рањивости, исправке, следљивост имовине и све одговорности за потребна координирања;*
- *најмање једном месечно, а по потреби и чешће, врши анализу дневника активности (activitylog, history, securitylog, transactionlog и др) у циљу идентификације потенцијалних слабости ИКТ система.*
- *за софтверске и друге технологије (засноване на списку имовине: видети 5.1) се одређују информациони ресурси за идентификовање одговарајућих техничких рањивости и за одржавање свести о истима; ови информациони ресурси се ажурирају на основу измена у инвентару или онда када се идентификују нови или други корисни ресурси;*

- *дефинише се временски распоред реаговања на обавештење о могућим техничким рањивостима;*
- *када је могућа техничка рањивост идентификована, тада се идентификују припадајући ризици и акције које треба предузети; такве акције могу да обухвате исправке рањивих система и/или примену других контрола;*
- *у зависности од тога колико хитно треба неку техничку рањивост узети у разматрање, предузете активности се спроводе у складу са контролама које су везане за управљање променама или спровођењем процедура за одговор на инциденте нарушавања безбедности (видети 27.5);*
- *ако је исправка доступна од легитимног извора, онда се оцењују ризици у вези са инсталирањем те исправке (ризике који настају услед рањивости треба упоредити са ризиком везаним за инсталирање исправке);*
- *исправке се морају прво испробати и вредновати пре него што се трајно угради, како би се осигурало да ће оне бити ефективне и да неће довести до споредних утицаја који се не могу толерисати; ако исправка није на располагању, онда треба размотрити друге контроле, као што су деактивирање услуга или могућности које се односе на рањивост, прилагођавање или додавање контрола приступа, (нпр. заштитну баријеру на границама мреже (видети 21.1)) или појачано надгледање како би се открили или спречили постојећи напади и утицало на повећање свести о рањивости;*
- *о свим предузетим процедурама се праве записи за проверу, а процес управљања техничким рањивостима треба редовно надгледати и вредновати како би се осигурале његова ефективност и ефикасност;*
- *најпре се узимају у разматрање системи са високим ризиком;*
- *ефективан процес управљања техничким рањивостима се усклађује са активностима које се односе на управљање инцидентима, тако да обезбеди техничке процедуре које треба спровести ако се догоди неки инцидент;*
- *креира се процедура која узима у обзир ситуацију у којој је идентификована рањивост, али не постоји погодна контрамера. У овој ситуацији, организација треба да процени ризик у односу на познате рањивости и дефинише одговарајуће мере за откривање, као и корективне мере.*

Уколико се идентификују рањивости које могу да угрозе безбедност ИКТ система, < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > је дужан да одмах изврши подешавања, односно инсталира софтвер који ће отклонити уочене рањивости. Прво се узимају у разматрање системи са високим ризиком.

Ограничења у погледу инсталације софтвера

Забрањено је инсталирање софтвера на уређајима који могу довести до изложености ИКТ система безбедносним ризицима.

< Посебним документом је дефинисано које врсте софтвера запослени сме да инсталира, а које су забрањене. >

Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система

Члан 25.

Приликом спровођења ревизије ИКТ система, < Оператор ИКТ система > обезбеђује да ревизија има што мањи утицај на фукционисање система.

#Поступак контроле информационих система:

- *Са руководством су договорени захтеви за проверу приступа систему и подацима;*
- *Предмет и подручје испитивања за проверу су унапред договорени и строго контролисани;*
- *Испитивања за проверу су ограничена на приступ читањем;*
- *Приступ који није ограничен само на читање треба дозволити само за добијање издвојених копија системских датотека које се по завршеној провери бришу или се одговарајући штите уколико постоји обавеза да се такве датотеке чувају према захтевима за документовање провере;*
- *Захтеви за посебну или допунску обраду морају бити идентификовани и о томе мора бити сачињен писани споразум;*
- *Испитивања за проверу могу утицати на доступност система, па се покрећу ван радног времена;*
- *Сав приступ се надгледа и записује се да би се направио референтни траг.*

Планираање и спровођење ревизије ИКТ система може да врши само < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >, односно запослени-корисник који има овлашћење за то.

Заштита података у комуникационим мрежама укључујући уређаје и водове

Члан 26.

У циљу заштите података у комуникационим мрежама, уређајима и водовима врши се њихова контрола и заштита од неовлашћеног приступа.

Спецификација мрежних услуга, било да се оне пружају унутар самог Оператора ИКТ система било од стране трећих лица, укључују механизме безбедности, врсте услуга утврђених на захтев руководства. Мрежне услуге обухватају обезбеђивање прикључака, услуге на приватним мрежама и мреже са додатним функцијама, као и решења за управљање безбедношћу (заштита и системи за откривање упада).

У мрежама су међусобно раздвојене групе информационих услуга, корисника и системи, а мрежни администратор је одговоран за управљање мрежом.

< Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > је дужан/а да стално врши контролни преглед мрежне опреме и благовремено предузима мере у циљу отклањања евентуалних неправилности.

Безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система

Члан 27.

Заштита података који се преносе комуникационим средствима унутар < Оператор ИКТ система >, између оператора ИКТ система и лица ван оператора ИКТ система, обезбеђује се утврђивањем одговарајућих правила, процедура, потписивањем уговора и споразума, као и применом адекватних контрола.

- Правила коришћења електронске поште

Употреба електронске поште мора бити у складу са успостављеним процедурама и адекватним контролама над спровођењем истих. Електронска пошта се може користити искључиво за пословне потребе; размена порука личног садржаја није дозвољена; сви подаци садржани у порукама или њиховом прилогу морају бити у складу са стандардима заштите података.

- Правила коришћења Интернета

Приступ садржајима на Интернету је дозвољен искључиво за пословне намене. На мрежи је омогућено надгледање, односно користи се поступак периодичне ревизије и контролисања логовања, како на пријему тако и на слању.

- Правила коришћења информационих ресурса

Информациони ресурси се користе искључиво у пословне сврхе, на раду или у вези са радом. Другу намену коришћења посебно одобрава одговорно лице, на образложени писани захтев корисника.

Споразуми о преносу информација

Безбедан пренос пословних информација између организације и трећег лица обезбеђује се поштовањем споразума о преносу информација.

#Споразуми о преносу информација треба да укључе следеће:

1. *одговорности руководства за контролу и извештавање о преносу, отпреми и пријему;*
2. *процедуре за обезбеђење следљивости и непорецивости;*
3. *минималне техничке стандарде за паковање и пренос;*
4. *стандарде за идентификовање курира;*
5. *обавезе и одговорности у случају инцидената нарушавања безбедности информација, као што је губитак података;*
6. *коришћење договореног система означавања осетљивих или критичних информација, уз осигуравање да је значење ознака одмах разумљиво и да су те информације заштићене на одговарајући начин;*
7. *посебне контроле које су потребне да би се заштитили осетљиви детаљи, попут криптографије;*
8. *одржавање ланца надзора за информације у току преноса.*

Размена електронских порука

Заштита информација укључених у размену електронских порука се регулише Процедуром о безбедности у размени електронских порука.

#Процедура о безбедности у размени електронских порука треба да обухвати:

- *заштиту порука од неовлашћеног приступа, модификовања или одбијања услуга које су у складу са класификационом шемом коју је усвојио Оператор ИКТ система;*
- *осигурање исправног адресирања и транспорта поруке;*
- *поштовање законских одредби, на пример захтеве за електронске потписе;*
- *добијање одобрења пре коришћења јавних спољних услуга, као што су размена хитних порука, приступ и коришћење друштвене мреже или заједничко коришћење датотека;*
- *строже нивое утврђивања веродостојности, контролисањем приступа из мрежа са јавним приступом.*

Споразуми о поверљивости или неоткривању

Споразуми о поверљивости или неоткривању имају за циљ заштиту информација < Оператор ИКТ система > и обавезују потписнике да информације штите, користе и објављују их на одговоран и ауторизован начин.

#Да би се идентификовали захтеви за споразуме о поверљивости или неоткривању, треба узети у обзир следеће елементе:

1. *дефиницију информација које треба заштитити;*
2. *очекивано трајање споразума, укључујући случајеве у којима је потребно да се поверљивост сачува неограничено;*
3. *поступања које се захтевају по истеку споразума, попут повраћаја или уништавања информација;*
4. *дозвољено коришћење поверљивих информација и пословних тајни, као и права потписника да користи информације;*
5. *право на проверу и праћење активности које укључују поверљиве информације;*
6. *процес за обавештавање и извештавање о неовлашћеном откривању или приступу поверљивим информацијама;*
7. *радње које треба предузети у случају кршења овог споразума.*

Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система

Члан 28.

У оквиру животног циклуса ИКТ система који укључује фазе конципирања, спецификације, пројектовања, развијања, тестирања, имплементације, коришћења, одржавања и на крају повлачења из употребе, < Оператор ИКТ система > је у обавези да обезбеди информациону безбедност у свакој фази. Питање безбедности се анализира у раним фазама пројеката информационих система јер такво разматрање доводи до ефективнијих и рационалнијих решења.

< Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > је задужен за технички надзор над реализацијом од стране извођача, односно испоручиоца.

О успостављању новог ИКТ система, односно увођењу нових делова и изменама постојећих делова ИКТ система < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > води документацију.

Документација из претходног става мора да садржи описе свих процедура, а посебно процедура које се односе на безбедност ИКТ система.

Анализа и спецификација захтева за информациону безбедност

У захтеве за нове информационе системе или за побољшање постојећих информационих система морају бити укључени захтеви који се односе на информациону безбедност и они су саставни део уговора о набавци, модификацији и одржавању информационог система.

Захтеви за информациону безбедност укључују:

- Проверу идентитета корисника;
- Доступност, поверљивост, непорецивост и интегритет података и имовине;
- Надгледање пословних процеса;
- Омогућавање приступа уз проверу веродостојности за пословне, привилеговане и техничке кориснике.

Спецификација захтева обухвата аутоматску контролу која ће бити уведена у информациони систем, као и потребу да постоји и ручна контрола, која мора бити примењена при вредновању развијених или купљених пакета софтвера, намењених за пословне апликације.

Системски захтеви за информациону безбедност и процеси за увођење безбедности се интегришу у фази дизајнирања информационих система.

Формално тестирање и процес имплементације ће се примењивати за све купљене производе.

У уговору са извођачем, односно испоручиоцем купљених производа, посебно се дефинишу захтеви за информациону безбедност.

У случају да безбедносна функционалност предложеног производа не задовољава одређен захтев, ризик и повезане контроле ће бити преиспитане пре куповине производа.

Обезбеђивање апликативних услуга у јавним мрежама

Информације обухваћене апликативним услугама које пролазе кроз јавне мреже треба заштити од малверзација, неовлашћеног откривања података и модификовања. Неопхнодно је потврдити идентитет корисника и извршити поделу овлашћења и одговорности за постављање садржаја, електронског потписивања или обављања трансакција.

Заштита трансакција апликативних услуга

Информације укључене у трансакције апликативних услуга се штите да би се спречио непотпун пренос, погрешно усмеравање, неовлашћено мењање порука, неовлашћено разоткривање, неовлашћено копирање порука или поновно емитовање.

<Трансакције морају да подрже следеће услове:

- Обе стране које учествују у транскакцији морају да примене електронски потпис;
- Приватност свих страна које учествују у трансакцији;
- На комуникационим каналима примењено шифровање;
- Безбедност протокола који се користе у трансакцијама.>

Заштита података који се користе за потребе тестирања ИКТ система односно делова система

Члан 29.

Под тестирањем ИКТ система, као и тестирањем делова система, подразумева се процена промене стања система, односно делова система, који су унапређени или изложени променама. Под процесом тестирања подразумева се процес употребе једног или више задатих објеката под посебним околностима, да би се упоредиле актуелна и очекивана понашања.

Тестирање ИКТ система, односно делова система, дозвољено је под условом потпуне примене свих безбедносних мера наведених у овом члану.

За потребе испитивања и тестирања ИКТ система, односно делова система, < Оператор ИКТ система > избегава коришћење оперативних података који садрже личне податке или било које друге поверљиве податке и информације на основу којих је могуће идентификовати појединачног добављача, купца, запосленог или др. Уколико се за сврху испитивања користе лични подаци или неке друге поверљиве информације, онда се сви осетљиви подаци и информације пре коришћења штите анонимизацијом личних података, уклањањем садржаја или изменом текста садржаја у предметном делу.

<Уколико је за тестирање неопходно користити оперативне податке, примењују се следеће смернице:

- за свако копирање оперативних података у тестно окружење се издаје посебно овлашћење;
- приликом тестирања апликативних система примењују се процедуре за контролу приступа које се примењују и на оперативним системима;
- оперативне информације се одмах по завршетку испитивања бришу из тестног окружења.>

За податке који су означени ознаком тајности, односно службености као поверљиви подаци, или су подаци о личности коришћени приликом тестирања система, одговоран је < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >, у складу са прописима којима је дефинисана употреба и заштита такве врсте података.

За потребе тестирања ИКТ система односно делова система < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > система може да користи податке који нису осетљиви, које штити, чува и контролише на одговарајући начин.

Приликом тестирања апликативних система примењују се додатне процедуре за контролу приступа путем физичке заштите и применом криптографских мера за заштиту система и података од неовлашћених приступа, а које се примењују и на оперативним системима. Скуп криптографских мера које ће бити примењене за заштиту података утврђује < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >, узимајући у обзир њихову поузданост исврсисходност.

Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга

Члан 30.

Политика безбедности размене информација у пословним односима са пружаоцима услуга и између независних пружалаца услуга

Уговори који се закључују са пружаоцима услуга који имају приступ информацијама, средствима или опреми за обраду информација < Оператор ИКТ система > морају садржати уговорну одредбу о заштити и чувању поверљивости информација, података и документације.

Пружаоци услуга имају право на приступ информацијама које су крајње неопходне за пружање предметне услуге која је уговорена са < Оператор ИКТ система >.

< Оператор ИКТ система > успоставља контролу безбедности информација које се односе на процесе и процедуре које ће спроводити пружаоци услуга:

- идентификовање и документовање врсте пружаоца услуга којима ће < Оператор ИКТ система > дозволити да приступ информацијама;
- стандардизовани процес за управљање односима између пружаоца услуга;
- дефинисање врста информација које ће различитим типовима пружаоца услуга бити дозвољено ради приступања, праћења и контроле приступа;
- минимални захтеви за безбедност информација за сваку врсту информација и врсту приступа;
- процеси и процедуре за праћење придржавања утврђених захтева за безбедност за сваку врсту добављача и врсту приступа;
- контроле за осигурање интегритета информација или обраде информација коју обезбеђује било која страна;
- поступање са инцидентима и непредвиђеним ситуацијама које су у вези са приступом пружаоца услуга, укључујући одговорности и организације и пружаоца услуга;
- управљање неопходним променама информација, опреме за обраду информација и свега осталог што треба да се премешта и осигурање да се безбедност информација одржава током прелазног периода.

Уговарање обавезе обезбеђивања безбедности у споразумима са пружаоцима услуга

Пре отпочињања преговора, потенцијални пружалац услуга у обавези је да потпише изјаву о поверљивости и заштити података, информација и документације, која садржи обавезу за пружаоца услуга да достављене или на други начин учињене доступним информације и подаци могу бити коришћени искључиво на начин претходно одобрен од стране < Оператор ИКТ система > , а за потребе извршења предмета преговора.

Потребно је да изјава о поверљивости, односно уговор о пружању услуга, садржи одредбу о поверљивости са јасно утврђеном обавезом и одговорношћу пружаоца услуге уз претњу раскида уговора и накнаде штете у корист < Оператора ИКТ система > у случају повреде ове одредбе.

 # Пример: "Сви подаци и информације садржани у овом Уговору о пружању услуга се сматрају поверљивим пословним подацима и не смеју бити саопштени или на други начин учињени доступним трећим лицима. Нарочито се сматрају поверљивим сви пословни подаци и информације које једна страна учини доступним другој уговорној страни ради извршења обавеза из овог уговора, уколико ти подаци нису јавно доступни нити су били претходно познати другој страни.

Свака уговорна страна се обавезује да податке и информације које јој буду учињене доступним у складу са овим уговором и обавезом извршења уговорених послова и обавеза, буду стављене на располагање и увид запосленима, уколико је то неопходно ради извршења обавеза из овог уговора.

Уговорне стране се нарочито обавезују да поступају обазриво са подацима о личности до којих могу доћи у поступку извршења услуга за оператора ИКТ система, као и да те податке чувају и поступају у свему у складу са прописима који уређују заштиту података о личности.

У случају повреде ове обавезе уговорна страна чији су подаци коришћени има право раскида уговора и право да захтева накнаду штете услед неовлашћеног коришћења података и информација друге стране."

Пружаоци услуга дужни су да захтеве < Оператора ИКТ система > у погледу безбедности информација прошире и на своје подуговараче за додатне услуге или производе.

< Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > је одговоран за контролу приступа и надзор над извршењем уговорених обавеза, као и за поштовање одредби правилника којима су такве активности дефинисане.

Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга

Члан 31.

У циљу одржавања и обезбеђивања уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга, < Оператор ИКТ система > успоставља мере надзора и заштите за време пружања услуга и након извршеног посла.

Праћење и преиспитивање извршења уговорених обавеза пружаоца услуга

< Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > редовно прати, анализира, преиспитује и проверава извршене услуге и усаглашеност са уговореним услугама, на следећи начин:

1. Надгледање и преиспитивање услуга се може вршити преко трећег лица;
2. Неопходно је да се поштују сви услови из споразума у вези са безбедношћу информација, као и да се спрече сви инциденти и проблеми нарушавања безбедности, те омогући управљање на одговарајући начин;
3. Врши се оцена квалитета извршења и саобразности уговорене услуге;
4. Пружалац услуге има уговорну обавезу да организује и припреми периодичне састанаке који ће обезбедити редовно извештавање < Оператор ИКТ система > и унапредити квалитет уговорених услуга, односно умањити потенцијалну штету или инциденте који могу настати у поступку извршења услуге или након почетка примене;

5. < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > одржава потпуну контролу над спровођењем услуга и осигурава увид у све осетљиве или критичне безбедносне информације и друга средства за обраду информација којима трећа страна приступа, које процесуира или којима управља;
6. < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > одржава увид у безбедносне активности кроз јасно дефинисан процес извештавања;
7. Преиспитује трагове провере и записа о догађајима у вези са безбедношћу код пружаоца услуга, односно оперативним проблемима, отказима, праћењу неисправности и сметњама у вези са испорученим услугама.

Приликом закључења уговора неопходно је јасно дефинисати квалитативне, оперативне и финансијске критеријуме оцене; утврдити поступак извештавања, праћења и поступања у складу са захтевима < Оператор ИКТ система > у поступку извршења уговорених услуга и извршити оцену извршених услуга и квалитета пружаоца услуга.

Приликом надзора над извршењем квалитета и саобразности уговорене услуге проверава се да ли пружалац услуге задовољава све критеријуме који су били од пресудног значаја приликом избора, укључујући обим и квалитет услуге, као и да се у току поступка извршења услуге може утицати на побољшање квалитета услуге или начина и обима извршења, у складу са утврђеним стварним потребама < Оператор ИКТ система >.

У поступку објективне евалуације квалитета и обима пружене услуге у односу на уговорену, потребно је прикупити све релевантне чињенице, податке и документацију у вези са извршењем услуге, као и прикупити податке од непосредних, крајњих, корисника у вези са предметом услуге. Евалуација се може извршити слањем упитника, разговором са изабраним појединцима или на основу анонимног анкетирања путем електронске поште.

Управљање променама уговорених услуга од стране пружаоца услуга

Уговором са пружаоцем услуга треба обезбедити могућност континуираног управљања променама уговорених услуга, укључујући одржавање и унапређење постојећих процедура и контролу безбедности информација.

Промене које се узимају у обзир су промене у споразумима са пружаоцима услуга, повећање обима текућих услуга које се нуде, као и промене које уводи < Оператор ИКТ система > ради имплементације нове или промењене апликације, система, контрола или процедура у циљу побољшања безбедности.

Превенција и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама

Члан 32.

Одговорност појединаца и поступак одговора на инциденте

Посебним процедурама се уређује начин одговора на инциденте нарушавања информационе безбедности и одређује особа овлашћена за контакт у случајевима нарушавања безбедности, као и контакт санадлежним органима.

#Потребне процедуре

- *процедуре за припрему и планирање одговора на инциденте;*
- *процедуре за надгледање, детекцију, анализу и извештавање о догађајима и инцидентима у вези са безбедношћу информација;*
- *процедуре за записивање активности у оквиру управљања инцидентима;*
- *процедуре за поступање са судским доказима;*
- *процедуре за оцењивање и одлучивање о догађајима у оквиру безбедности информација и оцењивање слабости у погледу безбедности информација;*
- *процедуре за одговарање на инциденте, опоравак од инцидента и комуникацију са екстерним или интерним особама или организацијама.*

< Оператор ИКТ система >, одређује < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >, чији је задатак да придржавајући се процедура одређених овим чланом, планирају, детектују, анализирају и информишу надлежне у току и након инцидента.

< Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > подразумева одговарајућа техничка знања како би на најбржи и одговарајућу начин могли да одговоре на безбедносне инциденте.

< Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > у циљу превенције од безбедносних ризика обезбеђује више (различитих и другачијих) мехнизама за комуникацију и координацију у случају нарушавања безбедности. Ови еханизми могу бити бити:обезбеђивање контакт информација (број телефона, електронска адреса) појединаца и чланова тима у оквиру организације и ван ње, систем за праћење проблема, шифровани софтвер који би био коришћен од стране појединаца у оквиру организације и спољашних странака, посебну осигурану просторију за чување података и складиштење поверљивог материјала.

У случају било каквог инцидента који може да угрози безбедност ресурса ИКТ система, запослени--корисник је дужан да о томе одмах обавести < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >.

Извештавање о догађајима у вези са безбедношћу информација

Сви запослени морају бити упознати са обавезом и процедуром извештавања о догађајима у вези са информационом безбедношћу.

< Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > је у дужан да припреми план и неколико метода комуникације које би могле да се примене у зависности од инцидента. Могуће методе комуникације су: електорнска пошта, веб сајтови (интерни, екстерни, портали), телефонска комуникација, говорна порука, писмено извештавање, директан контакт.

У случају погрешног функционисања или других аномалијских понашања система врши се исто извештавање као и у случају догађаја у вези са информационом безбедношћу

#Процедура:

1. *Запослени који сматра да је дошло до напада или злоупотребе података мора одмах припремити опис проблема и послати га електронском поштом сектору за информационе технологије (help desk)/ позвати број/ пријавити проблем путем Интернет стране за help desk;*
2. *Адресу електронске поште, број телефона и Интернет страну за help desk проверава систем администратор;*
3. *Систем администратор врши проверу пријављеног инцидента и даље поступа по одговарајућој процедури.*

Када је индетификован инцидент запослени је дужан да одмах обавести < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >, и предузме мере у циљу заштите ресурса ИКТ система.

< Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > води евиденцију о свим инцидентима, као и пријавама инцидената, у складу са уредбом, на основу које, против одговорног лица, могу да се воде дисциплински, прекршајни или кривични поступци.

Извештавање о утврђеним слабостима система заштите

Сви запослени су у обавези да о уоченим и утврђеним слабостима ИКТ система известе < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици >, у што краћем року, како би се инциденти нарушавања информационе безбедностиспречили и спречио настанак штете.

Одговорно лице за обавештавање надлежних органа о инцидентима у ИКТ систему који могу да имају значајан утицај на нарушавање информационе безбедности, поступа у складу са одговарајућом процедуром.

Догађаји у вези са информационом безбедношћу се оцењују и у складу са анализом се доноси одлука да ли је потребно да се класификују као инциденти нарушавања информационе безбедности.

Одговор на инциденте нарушавања информационе безбедноости

< Оператор ИКТ система > је у обавези да усвоји План за превенцију од безбедносних ризика.

#План за превенцију од безбедносних ризика садржи одговоре на питања ко треба да буде контактиран, када и како и које акције треба предузети моментално у случају одређеног напада?

- *Класификациона шема – детаљи о подацима који се налазе у систему, њихов ниво осетљивости и поверљивости.*
- *Листа услуга – попис свих услуга које < Оператор ИКТ система > пружа, рангиране по важности.*
- *План за backup и restore података – дефинише за које податке се ради backup, носаче података на које ће се снимати, где се носачи чувају и колико често се backup изводи. Дефинише и поступак за restore података.*
- *План за замену опреме: Садржи списак потребне опреме, рангиране по важности.*
- *Односи са јавношћу: Утврђена је одговорна особа задужена за одосе са јавношћу, као и упутство које информације је дозвољено јавно објавити у случају напада.*

Прикупљено знање из анализе и решавања инцидената који су нарушилиинформациону безбедност, < Оператор ИКТ система > користи да би се идентификовали инциденти који се понављају и смањила вероватноћа и утицај будућих инцидената.

Прикупљање доказа

< Оператор ИКТ система > дефинише и примењује процедуре за идентификацију, сакупљање, набавку и чување информација које могу да служе као доказ у случају покретања дисциплинског, прекршајног или кривичног поступка.

Мере које обезбеђују континуитет обављања посла у ванредним околностима

Члан 33.

< Оператор ИКТ система > примењује мере које обезбеђују континуитет обављања посла у ванредним околностима, како би ИКТ систем у што краћем року био у функционалном стању.

Планирање континуитета мера безбедности информација

Континуитет пословања се осигурава кроз План за обезбеђење континуитета пословања и План опоравка од нежељених догађаја ИКТ система.

#При изради Плана за обезбеђење континуитета пословања за хардверске компоненте ИКТ система треба обухватити следеће:

- *документацију за логички и физички дијаграм и копије пројеката;*
- *заштитне копије конфигурационих фајлова и оперативног система активних уређаја;*
- *постојање резервне опреме;*
- *унапред направљене конфигурације за различите сценарије;*
- *израду резервних копија.*

#При изради Плана опоравка од нежељених догађаја ИКТ система:

- *проценити најкритичније апликације, податке, конфигурационе фајлове и системски софтвер за који треба направити резервне копије;*
- *одредити место чувања копије;*
- *одредити нову локацији рада ИКТ система у случају немогућности рада на основној локацији/избор рачунара који ће привремено заменити сервер док се сервер не стави у функцију.;*
- *навести податке о тиму који ће бити ангажован на отклањању последица нежељених догађаја;*
- *одредити изворе непрекидног напајања електричном енергијом.*

Такође, при изради Плана опоравка од нежељених догађаја ИКТ система потребно је предвидети:

- *постојање документације за сервисе, апликације и базе података;*
- *процедуре инсталације и конфигурисања сервиса, апликација и база података;*
- *место чувања инсталација сервиса, апликација и база података и резервне копије података;*
- *податке о тиму који ће бити ангажован на отклањању последица нежељених догађаја;*
- *развијене и одобрене документоване планове, одговоре и процедуре за опоравак, детаљно наводећи како ће организација управљати догађајима који узрокују поремећаје и како ће одржавати своју безбедност информација.*

Имплементација континуитета безбедности информација

Да би се осигурао потребан ниво континуитета безбедности информација током ванредних ситуација, < Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > примењује процедуре и контроле описане у Плану за обезбеђење континуитета пословања.

< Назив радног места надлежног за послове ИКТ система које припада одговарајућој организационој јединици > редовно врши проверу усвојених процедура контроле континуитета безбедности информација, како би оне биле адекватне и ефективне током ванредних ситуација.

Провера се врши вежбањем и испитивањем знања и рутине приликом руковања процесима, процедурама и контролама, као и преиспитивањем ефективности мера безбедности информација у случају промене информационих система, процеса, процедуре и контроле безбедности информација.

III ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Посебна обавеза < Оператора ИКТ система >

Члан 34.

Обавеза < Оператора ИКТ система > је да најмање једном годишње изврши проверу ИКТ система и изврши евентуалне измене Акта о безбедности, у циљу провере адекватности предвиђених мера заштите, као и утврђених процедура, овлашћења и одговорности у ИКТ систему < Оператора ИКТ система >.

Ступање на снагу Акта о безбедности

Члан 35.

Овај Акт о безбедности ступа на снагу < x x x >.

ОДГОВОРНО ЛИЦЕ

Садржај

РЕПУБЛИКА СРБИЈА

РАТЕЛ

РЕГУЛАТОРНА АГЕНЦИЈА ЗА
ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ
И ПОШТАНСКЕ УСЛУГЕ

СРБ-ЦЕРТ